PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-252320
(43)Date of publication of application : 22.09.1997

(51)Int.Cl. H04L 12/56
G06F 13/00
H04B 7/00
H04B 7/26
H04H 1/00
H04H 1/08

(21)Application number : 08-059745
(22)Date of filing : 15.03.1996

(71)Applicant : SONY CORP
(72)Inventor : ISHII MAKOTO

(54) DATA TRANSMITTER AND ITS METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To conduct digital data transmission adopting the high} quality radio system for only specific users.
SOLUTION: An internet protocol(IP) packet 32 generated by an IP packet generating section 3 is ciphered by a ciphering section 33 and a medium access control(MAC) frame generating section 36 provides a MAC header to the ciphered packet and generates a MAC frame 37. Then a cyclic redundancy check(CRC) calculation section 38 generates a CRC code and adds it to the MAC frame 37 to generate a MAC frame 39. Then a section generating section 40 generates a section 41 of a moving picture experts group(MPEG)2 and divides it into transport packets 43 and sends the result from a server to a client via a communication satellite.

<hr size=2 width="100%" align=center>

CLAIMS

[Claim(s)]
[Claim 1]In data transmission equipment which performs data communications between a server and a client via a networkData can be transmitted to a client with radio system from a serverthe 1st data communication channel in which bidirectional data communications are possible between clientsand said serverCompared with said 1st data communication channeltransmission capacity has the 2nd big data communication channeland it said serverData transmission equipment which transmits data according to a demand from said client to said client via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.
[Claim 2]Said 1st data communication channel is a course which used a terrestrial communication network.
The data transmission equipment according to claim 1 which is the course for which said 2nd data communication channel used a communications satellite.

[Claim 3]The data transmission equipment according to claim 1 in which said Internet Protocol is a TCP/IP protocol.
[Claim 4]The data transmission equipment according to claim 3 which said server changes data to transmit into an IP packetand transmits this IP packet to said client via said 2nd communication path.
[Claim 5]The data transmission equipment according to claim 4 which said server generates a MAC frame by media access control (MAC) from said IP packetand transmits this MAC frame to said client via said 2nd communication path.
[Claim 6]The data transmission equipment according to claim 5 which said server enciphers said IP packet and generates said one MAC frame about said one enciphered IP packet.
[Claim 7]An IP address of a client which should receive data in a header of said MAC frameA control bit for distinguishing whether data is media data according to a demand from a clientor it is the control data for system management from a control bit which shows existence of a data encryptionThe data transmission equipment according to claim 5 with which a bit which shows attached data length at the time of normalizing data length which is needed for enciphering data is contained.
[Claim 8]A means to encipher an IP packet which distributes said server to said client which advanced a demand by a peculiar encryption algorithm which only server concerned and the client concerned get to knowA means to create a MAC frame from said enciphered IP packet using media access controlA means to change into a section into which said MAC frame was specified by MPEG 2The data transmission equipment according to claim 4 which has a means to change said section into a transport stream to which it was specified by MPEG 2and a means to transmit said transport stream to said client via said 2nd communication path.
[Claim 9]The data transmission equipment according to claim 5 in which said server

and said client have further a means to inspect all the data bytes of said MAC framewith a CRC method.
[Claim 10]The data transmission equipment according to claim 5 which has further a means by which said server adds a CRC inspection bit about a MAC frame to the last of a MAC frame.
[Claim 11]The data transmission equipment according to claim 9 which has further a means by which said server adds a CRC inspection bit about a MAC frame to the last of a MAC frame.
[Claim 12]In a data distribution device which performs data communications between Kula and Yingde via a networkData can be transmitted to a client with radio system from the 1st interface connected with the data distribution device concerned at the 1st data communication channel in which bidirectional data communications are possible between clientsand the data distribution device concernedIt has the 2nd interface connected to the 2nd data communication channel with big transmission capacity compared with said 1st data communication channelA data distribution device which transmits data according to a demand from said client to said client via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.
[Claim 13]The data distribution device according to claim 12 which changes data to transmit into an IP packet and transmits this IP packet to said client via said 2nd communication path.
[Claim 14]The data distribution device according to claim 13 which enciphers said IP packetgenerates a MAC frame by said one media access controland transmits the MAC frame concerned about said one enciphered IP packet.
[Claim 15]A means to encipher an IP packet distributed to said client which advanced a demand by a peculiar encryption algorithm which only data distribution device concerned and the client concerned get to knowA means to create a MAC frame from said enciphered IP packet using media access controlA means to change into a section into which said MAC frame was specified by MPEG 2The data distribution device according to claim 14 which has a means to change said section into a transport stream to which it was specified by MPEG 2and a means to transmit said transport stream to said client via said 2nd communication path.
[Claim 16]In a data receiver which performs data communications between servers via a networkData can be transmitted to the data receiver concerned with radio system from the 1st interface connected to the 1st data communication channel in which bidirectional data communications are possible between said server and the data receiver concernedand said serverIt has the 2nd interface connected to the 2nd data communication channel with big transmission capacity compared with said 1st data communication channelA data receiver which receives data from said server via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.

[Claim 17]The data receiver according to claim 16 in which said data to receive is data of IP packet form.
[Claim 18]The data receiver according to claim 17 which incorporates a required IP packet selectively based on a header of a MAC frame by media access control contained in said data to receive.
[Claim 19]Are a data transmission method characterized by comprising the following which performs data communications between a server and a client via a networkand said serverA data transmission method which transmits data according to a demand from said client to said client via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.
The 1st data communication channel in which bidirectional data communications are possible between a server and a client.
The 2nd data communication channel with big transmission capacity compared with said 1st data communication channel that can transmit data to a client with radio system from said server.

[Claim 20]The data transmission method according to claim 19 which said 1st data communication channel is a course which used a terrestrial communication networkand is the course for which said 2nd data communication channel used a communications satellite.
[Claim 21]The data transmission method according to claim 19 in which said Internet Protocol is a TCP/IP protocol.
[Claim 22]The data transmission method according to claim 21 which said server changes data to transmit into an IP packetand transmits this IP packet to said client via said 2nd communication path.
[Claim 23]The data transmission method according to claim 22 which said server generates a MAC frame by media access control (MAC) from said IP packetand transmits this MAC frame to said client via said 2nd communication path.
[Claim 24]The data transmission method according to claim 23 which said server enciphers said IP packet and generates said one MAC frame about said one enciphered IP packet.
[Claim 25]An IP address of a client which should receive data in a header of said MAC frameA control bit for distinguishing whether data is media data according to a demand from a clientor it is the control data for system management from a control bit which shows existence of a data encryptionThe data transmission method according to claim 23 with which a bit which shows attached data length at the time of normalizing data length which is needed for enciphering data is contained.
[Claim 26]The data transmission method comprising according to claim 22:
A means to encipher an IP packet which distributes said server to said client which advanced a demand by a peculiar encryption algorithm which only server concerned

and the client concerned get to know.
A means to create a MAC frame from said enciphered IP packet using media access control.
A means to change into a section into which said MAC frame was specified by MPEG 2.
A means to change said section into a transport stream to which it was specified by MPEG 2and a means to transmit said transport stream to said client via said 2nd communication path.

[Claim 27]The data transmission method according to claim 23 in which said server and said client have further a means to inspect all the data bytes of said MAC framewith a CRC method.
[Claim 28]The data transmission method according to claim 23 which has further a means by which said server adds a CRC inspection bit about a MAC frame to the last of a MAC frame.
[Claim 29]The data transmission method according to claim 27 which has further a means by which said server adds a CRC inspection bit about a MAC frame to the last of a MAC frame.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to data transmission equipment for offering multimedia data distribution serviceand a method for the samefor example using a communications satellite.
[0002]
[Description of the Prior Art]Conventionallyin the data distribution service using communications satellitessuch as television broadcastingdata flow was only one way from a data distribution person to a user. In recent yearsit came to be transmitted by transmission of the digital data using a communications satellite having been attained using the communications satellite also about the textand the digital image and voice data which are used not only by analog video and voice datasuch as television and a moviebut by computer etc. Herethe conventional data distribution service using communications satellitessuch as television broadcastingis a gestalt as for which many users use the data which the data distribution person distributed receiving simultaneously. On the other handwhen distributing the digital data used by computer etc. via a communications satellitethe function which distributes data to the specific user of the singular number or plurality from a data distribution person is called for.
[0003]

[Problem(s) to be Solved by the Invention]Howeverin the conventional transmission system using a communications satellitesince it being distribution of analog data and data distribution are only one way from a data distribution person to a usera check function is not provided with the error on transmissionbut there is a problem that the reliability of data communications is low. In distribution of digital dataif at least 1 bit of errors arise to data by transmissionthe received data will become meaningless. In order to distribute such digital computer data with high quality with radio systemit is necessary to secure the channel not only from a user to the data distribution of one way from a data distribution person to a user but a data distribution person butand in the conventional transmission systemit does not have such a function.
[0004]In the conventional simultaneous transmissive communication or broadcasting system from a data distribution person to many usersAll Users receives the always same informationuse or an inspection is carried outand since there is no identification information of a system user individualthere is a problem that distribution of data only to a specific user from a data distribution person cannot be performed.
[0005]It aims at providing data transmission equipment which can transmit digital data with radio systemand a method for the samewithout making this invention in view of the problem of the conventional technology mentioned aboveand generating the error on transmission. An object of this invention is to provide data transmission equipment which can transmit digital data only to a specific client with radio systemand a method for the same.
[0006]
[Means for Solving the Problem]In order to attain the purpose mentioned abovedata transmission equipment of this inventionData can be transmitted to a client with radio system from a serverthe 1st data communication channel in which bidirectional data communications are possible between clientsand said serverCompared with said 1st data communication channeltransmission capacity has the 2nd big data communication channeland it said serverBased on Internet Protocol for transmitting and receiving digital data via a network between two or more systemsdata according to a demand from said client is transmitted to said client via said 2nd data communication channel.
[0007]The data transmission method of this invention can transmit data to a client with radio system from a serverthe 1st data communication channel in which bidirectional data communications are possible between clientsand said serverIt is a data transmission method which performs data communications between a server and a client via a network which has the 2nd data communication channel with big transmission capacity compared with said 1st data communication channelSaid server transmits data according to a demand from said client to said client via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.
[0008]In data transmission equipment of this inventionand a method for the same. For

examplein [if a client performs a predetermined request to a server via the 1st data communication channel] a serverData according to the request concerned is changed based on Internet Protocoland this changed digital data is transmitted to a client via the 2nd data communication channel.
[0009]According to data transmission equipment by this inventionand a method for the sametransmission becomes possible from a server with high quality about large scale digital data at a clientand transmission of digital data is further attained from a server only at a specific user.
[0010]
[Embodiment of the Invention]Data transmission equipment (information service system) concerning the embodiment of this invention and a method for the same are explained. The outline of the data transmission equipment for realizing data service which distributes the digital data (an imagea sounda textetc.) of multimedia is shown in drawing 1. In the data transmission equipment shown in drawing 1the data donor A owns the data distribution device 4 as a serverand the user B owns the data receiver 5 as a client. The data distribution device 4 and the data receiver 5 can communicate mutually via ISDN3 in which bidirectional communication is possible. Mass communication is possible at radio system via the communications satellite 2 to the data receiver 5 from the data distribution device 4.
[0011]The data flow in the data transmission equipment shown in drawing 1 is explained. It is assumed that the user B has signed the contract of delivery of multimedia data with the user donor A beforehand. Under the present circumstancesit is assumed that the user's B data receiver 5 is equipped with the function in which data is receivable from the data donor's A data distribution device 4. The data donor A knows that the contract with the user B is made beforehand.
[0012]Firstthe user B sends the request 6 of the purport that he would like to receive the predetermined service which the data donor A provides to the data donor Afor example via ISDN3 as a terrestrial communication network. The method in particular of sending this RIESUTO 6 may not be limitedbut may be decided by the kind of dataor a contract state with a userfor examplemail etc. may be sufficient as it. In accordance with a contractthe data donor A may provide service beforehandwithout sending the request 6.
[0013]The request 6 from the user B sent to the data distribution device 4 is received by the data request reception part 7and is sent to the data management part 9. The data management part 9 will perform the read request 10 of data to the data storing section 11if the contract information and the request 6 of the user B check that it is that meaningful and it is satisfactory. The data storing section 11 sends the multimedia data 12 to the data creation part 13having corresponded to the data read demand 10. In the data creation part 13to the multimedia data 12 from the data storing section 11IP-packet-izingEncryption and MAC (Media Access Control) which were beforehand decided peculiar to the user B Format conversion of the data

of frame-izingtransport-izing of MPEG(Moving Picutre Experts Group) 2etc. is performed. It mentions later about this data format conversion.
[0014]The multimedia data 12 from the data storing section 11 is sent to the communications satellite 2 by the data creation part 13 as the data 14creation or after format conversion is carried out. The data 14 sent via the communications satellite 2 can be received by all the users who are in the situation where not only the user's B data receiver 5 but data is receivable. The data receiver 5 receives all the data from the communications satellite 2and sorts out and receives the data according to the request 6 which he advanced from the inside.
[0015]That isthe data receiver 5 receives the data 14 of a large number containing the transmitted data according to the request 6 by the data receiving section 16. The data receiver 5 sorts out the data addressed to itselfthe data which he should receiveand the data (this is based also on a contract) which he can receive from the inside. This sorting is performed in the data selection part 18 of the data receiver 5. The data receiver 5 which the user B has is beforehand determined by the contract of the user B and the data donor A. Thereforethe characteristic data of other addressing to a user cannot be sorted out using the data receiver 5 which the user B has.
[0016]In the data selection part 18the data 19 in which what the user B receives is possible is altogether sent to the data decomposition part 20. The data addressed to user B sent to the data decomposition part 20 is disassembled or decodedturns into the multimedia data 21and is sent to the data execution part 22. By thisthe user B can receive the data addressed to user B which the user B requestedand this data service is completed. It may be continued over the case where reception of the requested data is performed among instantsand a long period of time. When it is data of the kind which it continues receiving over a long period of timereception of data will be succeedingly repeated within the user's B data receiver 5. This changes a situation according to the kind of data which the user B requested. The above is a series of data flow of the data transmission equipment by this invention.
[0017]The data format conversion of distributes data in the data distribution device 4next the data distribution device 4 is explained in detail. Firstthe data creation part 13 of the data donor's A data distribution device 4 is explainedreferring to drawing 2. It is accumulated in the data storing section 11 in the data distribution device 4 in the form where no multimedia data which a user needs is processed. The data storing section 11 told that the read request 10 of data came from the user B from the data management part 9 sends simultaneously the multimedia data 12 and the user's B Recipient information 30 which were requested to the IP packet preparing part 31 in the data creation part 13. In the user's B Recipient information 30it is an IP address required for IP packet transmission here. The data transmission equipment concerning this embodiment has assigned the IP address peculiar to all the contract users. While the user B has secured the IP address which the user B hasno users other than the

user B have.
[0018]The multimedia data 12 and IP address 30 addressed to user B which were sent from the data storing section 11 are sent to the IP packet preparing part 31. At the IP packet preparing part 31IP packet 32 is generated using IP address 30 which specifies the user B at the multimedia data 12 sent from the data storing section 11and its time. The size of this IP packet is prescribed by TCP/IP (Transmission Control Protocol/Internet Protocol)When the multimedia data which the user B requested exceeds that sizethis multimedia data is divided into two or more IP packetsand is transmitted to the following cryptopart 33.
[0019]The format of IP packet 32 used in the data transmission equipment concerning this embodiment is shown in drawing 4. Detailed explanation of each control bit in the IP header in an IP packet is omitted here. Howeverthe IP address which the user's B data receiver 5 has goes into the area of transmission destination IP address 61 in IP blanketand the IP address of the data donor's A data distribution device 4 goes into the area of transmitting agency IP address 60. The multimedia data 12 from the data storing section 11 in drawing 2 goes into the data division 53 in drawing 4.
[0020]IP packet 32 created by the IP packet preparing part 31 shown in drawing 2 is transmitted to the cryptopart 33. In the cryptopart 33it gets to know that Recipient is the user B by transmission destination IP address 61 in IP packet 32and the IP packet whole [32] is enciphered with the secret key which already becomes acquainted only between the data donor A and the user B at the time. As a cipher systemDES (Data EncryptionStandard) etc. are adoptedfor example. Since the IP address which the user B uses is included in the header of IP packet 32 hereit seems that it is not necessary to encipher with the secret key only for user Bbut. This is needed in order to prevent others' impersonating the user B using the user's B IP addressand using by stealth the data addressed to user B.
[0021]Howeverencryption does not encipher all the data to the user Band encryption may not be performed depending on the kind of data. When encryption is not performedIP packet 32 is directly transmitted to the MAC frame preparing part 36 from the IP packet preparing part 31. This embodiment describes the case where encryption is performed. Encryption is usually performed to a 64-bit plaintextand in not being a multiple whose data length of IP packet 32 which should be enciphered is 64 bitsit makes the whole IP packet into a 64-bit multiple by performing amends of datai.e.the padding of invalid data.
[0022]The packet data 35 in which the IP packet 32 whole addressed to user B was enciphered are transmitted to the MAC frame preparing part 36. The format of MAC frame 37 is shown in drawing 5. In the MAC frame preparing part 36MAC header 119 as shown in drawing 5 is added to IP packet 35 addressed to user B enciphered by the cryptopart 33. Transmission destination IP address 54 in MAC header 119 is an IP address which the user B has. Herethe transmission destination IP address in enciphered IP packet 35 is the same as transmission destination IP address 54 of

MAC header 119. ThusMAC header 119 is attached because the data receiver 5 can know a transmission destination IP address only from MAC header 119 at the time of data receiving. That issince the user B cannot see a transmission destination addresshe cannot identify whether it is a packet addressed to itself only by the enciphered packet 35until the data receiver 5 decodes the IP packet 35 enciphered whole. Thereforebefore the data receiver 5 decodes the IP packet which receivedin order for the IP packet to know that it is a thing addressed to itselftransmission destination IP address 54 needs to be set to the header of a MAC frame. This transmission destination IP address 54 is directly passed to the MAC frame preparing part 36 from the IP packet preparing part 31.

[0023]PBL55 in MAC header 119 shown in drawing 5 is padding byte lengthand is the length of the invalid data covered on the occasion of encryption. This is needed in order that the user who received the enciphered IP packet may know regular data length. CP56 is a bit which identifies whether the multimedia data which a user needsor control data required for system management is contained in the IP packet. UsuallyCP56 of MAC frame 37 which should be received when a user requests shows that not control data but multimedia data is contained. EN57 in MAC header 119 is a control bit which shows whether the IP packet was enciphered by the cryptopart 33. As for a userdecoding received MAC frame 37 determines whether lends and there is by this bit information. In the MAC frame preparing part 36 of drawing 2it is added to IP packet (encryption is not carried out depending on the case) 35 as which the above control bit was enciphered.

[0024]MAC frame 37 generated by the MAC frame preparing part 36 of drawing 2 is transmitted to the CRC calculation part 38. In the CRC calculation part 38a MAC frame 37 all byte's CRC (Cyclic RedundancyChecking: Cyclic Redundancy Check) which has been sent is calculated. In this embodimentCRC is 16 bits. Thusby calculating CRCthe data receiver 5 can inspect whether the received MAC frame is correctly transmitted from the communications satellite 2. 16-bit CRC38a generated in the CRC calculation part 38 is added to the last of MAC frame 37as shown in drawing 3 and drawing 5.

[0025]MAC frame 39 to which CRC38a was added is changed into the section which is transmitted to the section preparing part 40 and specified by MPEG 2. As shown in drawing 3MAC frame 39 is added immediately after the section header (SecHd) 120. The format of the section header 120 is shown in drawing 6 (A). The format of the section header 120 shown by drawing 6 (A)It is prescribed by MPEG 2 and has table id100the section sink indicator 101the private indicator 102reserved one 103and the private section length 104. Herethe data length of MAC frame 39 goes into the private section length 104.

[0026]The section 41 created by the section preparing part 40 shown in drawing 2 is transmitted to the transport packet preparing part 42. In the transport packet preparing part 42the transmitted section format data is divided into the transport

packet 43and it transmits to the following data transfer part 44.
[0027]The format of the packet header (TSHd) 121 of the transport packet 43 shown in drawing 3 is shown in drawing 6 (B). The header format of the transport packet 43 is prescribed by MPEG 2. As shown in drawing 6 (B)the packet header 121 of the transport packet 43The sync byte 110the transport error indicator 111the pay-load unit start indicator 112the transport priority 113PID114the transport scramble control 115It has the adaptation field control 116 and the Conti ******- counter 117. Since the size for one piece of the transport packet 43 is specified as 188 bytesgenerally it is necessary to divide the one section 41 into two or more transport packets 43.
[0028]Since one section is not necessarily the integral multiple length of 184 bytes (number of bytes which subtracted 4 bytes of header length from 188 bytes)usually hereWhen dividing the one section 41 into two or more transport packets 43as shown in drawing 3data stopgap called stuffing is performed and the stuffing field 51 is formed. That iswhen the one section 41 which is not 184 bytes of multiple is divided into two or more transport packets 43all the bits 1 form the stuffing field 51 by which stuffing was carried out in the data area in which the last transport packet 43 remained.
[0029]Thusafter being transmitted to the data transfer part 44 and passing along data processing partssuch as a multiplexerthe section 41 divided into two or more transport packets 43 is transmitted to the communications satellite 2and is broadcast. The multimedia data for the broadcast user B will be received by the user's B data receiver 5reverse processing shown by drawing 2 will be performed by the data decomposition part 20and the multimedia data requested eventually will arrive to the user B3.
Data receiver 5[0030]fundamentallythe concrete processing performed in the data decomposition part 20 of the data receiver 5 of the user B who shows drawing 2 can be set in the data creation part 13 of the data distribution device 4and is a reverse algorithm of an algorithm. Firstin the data receiving section 16 shown in drawing 1the transport packet 43 shown in drawing 3 which received via the communications satellite 2 is combinedand the section 41 is generated. Nextthe data receiving section 16 elongates the section 41generates MAC frame 39and outputs this to the data selection part 18. And in the data separation part 18it is judged whether this transmission destination IP address 54 and the IP address of the data receiver 5 are in agreement based on transmission destination IP address 54 shown in drawing 5 contained in the Mac header 119 of MAC frame 39 shown in drawing 3. And the data separation part 18 sorts out the data concerned to a caseand the bottom in agreement outputs it to the data decomposition part 20 as the data 19 which shows drawing 1 enciphered IP packet 35 which is shown in drawing 3 contained in this data.
[0031]In the data decomposition part 20after carrying out the double sign of enciphered IP packet 35 which is shown in drawing 3 inputted as the data 19 using the secret key which becomes acquainted only about between the data donors A

beforehanda data error inspection etc. are conducted. Herewhen there is a data errorthe data which performs processing to which data is returned or has the error concerned is canceledfor example.
[0032]As explained aboveaccording to data transmission equipment concerning this embodimentand a method for the sameuse a TCP/IP communications protocoland. By providing a CRC bit in an IP packeteven when digital data is transmitted to the data receiver 5 via the communications satellite 2 from the data distribution device 4it controls effectively that a data transmission error occursand quality digital data transmission can be realized. According to data transmission equipment concerning this embodimentand a method for the samedata can be transmitted only to a specific user by transmitting an IP packet by a MAC frame method. According to data transmission equipment concerning this embodimentand a method for the samethe data transmitted is encipheredand since only the data receiver 5 has a secret key which decrypts itthe data concerned can prevent embezzling for others effectively.
[0033]This invention is not limited to the embodiment mentioned above. For examplethe data compression method of a MAC frame is not limited to MPEG 2but other compression methods may be used for it. Internet Protocol is not limited to TCP/IPfor examplean OSI (Open Systems Interconnection) method may be used for it. although illustrated about the case where a secret key is usedas an encryption method in this embodimentthe same effect is acquired even if it uses a public key -- things can be carried out.
[0034]
[Effect of the Invention]According to data transmission equipment of this inventionand a method for the sameeven when transmitting data with radio systemit controls effectively that a data transmission error occursand quality digital data transmission can be realized. According to data transmission equipment of this inventionand a method for the samedata can be transmitted only not only to broadcast type data distribution but to the specific user of the singular number or plurality with radio system by adopting a MAC frame method. According to data transmission equipment of this inventionand a method for the samethe data concerned can prevent embezzling for others effectively by transmitting the enciphered data. The data transmission equipment which has the effect which was mentioned above is realizable by using the data distribution device and data receiver of this invention.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a lineblock diagram of the data transmission equipment concerning the embodiment of this invention.

[Drawing 2]It is a lineblock diagram of the data distribution device shown in drawing 1.
[Drawing 3]It is a figure for explaining the processing in the data distribution device and data receiver which are shown in drawing 2.
[Drawing 4]It is a figure for explaining the format of an IP packet.
[Drawing 5]It is a figure for explaining the format of a MAC frame.
[Drawing 6](A) is a figure for explaining the format of a section header (SecHd)and (B) is a figure for explaining the packet header (TSHd) of a transport packet.
[Description of Notations]
2 [-- Data receiver] -- A communications satellite3 -- ISDN4 -- A data distribution device5 6 [-- Data read demand] -- A request7 -- A request reception part9 -- A data management part10 11 -- A data storing section12 -- Multimedia data13 -- Data creation part14 -- The data16 which are transmitted with radio system -- A data receiving section18 -- Data selection part19 -- The data which the user B can receive20 -- Data decomposition part21 -- Multimedia data22 -- A data execution part31 -- IP packet preparing part33 -- A cryptopart26 -- A MAC frame preparing part38 -- CRC calculation part40 [-- An IP packet35 / -- The IP packet39 which were enciphered / -- A MAC frame120 / -- A section header121 / -- A transport packet header43 / -- Transport packet] -- A section preparing part42 -- A transport packet preparing part44 -- A data transfer part32

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－252320

(43)公開日　平成９年(1997)９月22日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/56		9466－5K	Ｈ０４Ｌ	11/20	１０２Ａ
Ｇ０６Ｆ	13/00	３５１		Ｇ０６Ｆ	13/00	３５１Ｌ
Ｈ０４Ｂ	7/00			Ｈ０４Ｂ	7/00	
	7/26			Ｈ０４Ｈ	1/00	Ｈ
Ｈ０４Ｈ	1/00				1/08	

審査請求　未請求　請求項の数29　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平8－59745

(22)出願日　平成８年(1996)３月15日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　石井　眞
東京都品川区北品川６丁目７番35号　ソニー株式会社内

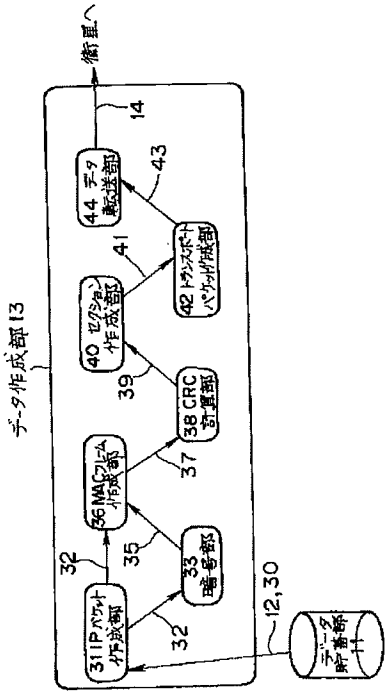
(74)代理人　弁理士　佐藤　隆久

(54)【発明の名称】　データ伝送装置およびその方法

(57)【要約】

【課題】　高品質な無線方式のディジタルデータ伝送を、特定のユーザのみに行うことができるデータ伝送装置およびその方法を提供する。

【解決手段】　ＩＰパケット作成部３４で生成されたＩＰパケット３２を暗号部３３で暗号化し、ＭＡＣフレーム作成部３６においてＭＡＣヘッダを付けてＭＡＣフレーム３７を生成する。次に、ＣＲＣ計算部３８でＣＲＣを形成し、これをＭＡＣフレーム３７に付加してＭＡＣフレーム３９を生成する。次に、セクション作成部４０でＭＰＥＧ２のセックション４１を作成し、これをトランスポートパケット４３に分割した後に、通信衛星を介して、サーバからクライアントに送信する。



【特許請求の範囲】
【請求項１】サーバとクライアント間のデータ伝送をネットワークを介して行うデータ伝送装置において、
サーバとクライアント間で双方向のデータ伝送が可能な第１のデータ通信経路と、
前記サーバからクライアントにデータを無線方式で伝送可能で、前記第１のデータ通信経路に比べて伝送容量が大きな第２のデータ通信経路とを有し、
前記サーバは、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第２のデータ通信経路を介して前記クライアントに伝送するデータ伝送装置。
【請求項２】前記第１のデータ通信経路は、地上通信網を用いた経路であり、
前記第２のデータ通信経路は、通信衛星を用いた経路である請求項１に記載のデータ伝送装置。
【請求項３】前記インターネットプロトコルは、ＴＣＰ／ＩＰプロトコルである請求項１に記載のデータ伝送装置。
【請求項４】前記サーバは、伝送するデータをＩＰパケットに変換し、このＩＰパケットを、前記第２の通信経路を介して前記クライアントに伝送する請求項３に記載のデータ伝送装置。
【請求項５】前記サーバは、前記ＩＰパケットからメディアアクセス制御（ＭＡＣ）によってＭＡＣフレームを生成し、このＭＡＣフレームを、前記第２の通信経路を介して前記クライアントに伝送する請求項４に記載のデータ伝送装置。
【請求項６】前記サーバは、前記ＩＰパケットを暗号化し、暗号化された１個の前記ＩＰパケットについて、１個の前記ＭＡＣフレームを生成する請求項５に記載のデータ伝送装置。
【請求項７】前記ＭＡＣフレームのヘッダには、
データを受け取るべきクライアントのＩＰアドレスと、
データの暗号化の有無を示す制御ビットと、
データが、クライアントからの要求に応じたメディアデータであるか、あるいはシステム運用のための制御データであるかを区別するための制御ビットと、
データを暗号化するのに必要となるデータ長の正規化を行なった際の付加データ長を示すビットとが含まれる請求項５に記載のデータ伝送装置。
【請求項８】前記サーバは、
要求を出した前記クライアントに配信するＩＰパケットを、当該サーバおよび当該クライアントのみが知る固有の暗号化アルゴリズムによって暗号化する手段と、
メディアアクセス制御を用いて、前記暗号化されたＩＰパケットからＭＡＣフレームを作成する手段と、
前記ＭＡＣフレームをＭＰＥＧ２で規定されたセクションに変換する手段と、
前記セクションを、ＭＰＥＧ２で規定されたトランスポートストリームに変換する手段と、
前記トランスポートストリームを前記第２の通信経路を介して前記クライアントに伝送する手段とを有する請求項４に記載のデータ伝送装置。
【請求項９】前記サーバおよび前記クライアントは、ＣＲＣ方式によって、前記ＭＡＣフレームの全データバイトを検査する手段をさらに有する請求項５に記載のデータ伝送装置。
【請求項１０】前記サーバは、ＭＡＣフレームについてのＣＲＣ検査ビットを、ＭＡＣフレームの最後に付加する手段をさらに有する請求項５に記載のデータ伝送装置。
【請求項１１】前記サーバは、ＭＡＣフレームについてのＣＲＣ検査ビットを、ＭＡＣフレームの最後に付加する手段をさらに有する請求項９に記載のデータ伝送装置。
【請求項１２】クライントとの間のデータ伝送をネットワークを介して行うデータ配信装置において、
当該データ配信装置とクライアント間で双方向のデータ伝送が可能な第１のデータ通信経路に接続された第１のインターフェースと、
当該データ配信装置からクライアントにデータを無線方式で伝送可能で、前記第１のデータ通信経路に比べて伝送容量が大きな第２のデータ通信経路に接続された第２のインターフェースとを有し、
複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第２のデータ通信経路を介して前記クライアントに伝送するデータ配信装置。
【請求項１３】送信するデータをＩＰパケットに変換し、このＩＰパケットを、前記第２の通信経路を介して前記クライアントに伝送する請求項１２に記載のデータ配信装置。
【請求項１４】前記ＩＰパケットを暗号化し、暗号化された１個の前記ＩＰパケットについて、１個の前記メディアアクセス制御によるＭＡＣフレームを生成し、当該ＭＡＣフレームを伝送する請求項１３に記載のデータ配信装置。
【請求項１５】要求を出した前記クライアントに配信するＩＰパケットを、当該データ配信装置および当該クライアントのみが知る固有の暗号化アルゴリズムによって暗号化する手段と、
メディアアクセス制御を用いて、前記暗号化されたＩＰパケットからＭＡＣフレームを作成する手段と、
前記ＭＡＣフレームをＭＰＥＧ２で規定されたセクションに変換する手段と、
前記セクションを、ＭＰＥＧ２で規定されたトランスポートストリームに変換する手段と、

前記トランスポートストリームを前記第２の通信経路を介して前記クライアントに伝送する手段とを有する請求項１４に記載のデータ配信装置。

【請求項１６】サーバとの間のデータ伝送をネットワークを介して行うデータ受信装置において、

前記サーバと当該データ受信装置間で双方向のデータ伝送が可能な第１のデータ通信経路に接続された第１のインターフェースと、

前記サーバから当該データ受信装置にデータを無線方式で伝送可能で、前記第１のデータ通信経路に比べて伝送容量が大きな第２のデータ通信経路に接続された第２のインターフェースとを有し、

複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記サーバからのデータを、前記第２のデータ通信経路を介して受信するデータ受信装置。

【請求項１７】前記受信するデータは、ＩＰパケット形式のデータである請求項１６に記載のデータ受信装置。

【請求項１８】前記受信するデータに含まれるメディアアクセス制御によるＭＡＣフレームのヘッダに基づいて、必要なＩＰパケットを選択的に取り込む請求項１７に記載のデータ受信装置。

【請求項１９】サーバとクライアント間で双方向のデータ伝送が可能な第１のデータ通信経路と、前記サーバからクライアントにデータを無線方式で伝送可能で、前記第１のデータ通信経路に比べて伝送容量が大きな第２のデータ通信経路とを有するネットワークを介してサーバとクライアント間のデータ伝送を行うデータ伝送方法であって、

前記サーバは、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第２のデータ通信経路を介して前記クライアントに伝送するデータ伝送方法。

【請求項２０】前記第１のデータ通信経路は、地上通信網を用いた経路であり、

前記第２のデータ通信経路は、通信衛星を用いた経路である請求項１９に記載のデータ伝送方法。

【請求項２１】前記インターネットプロトコルは、ＴＣＰ／ＩＰプロトコルである請求項１９に記載のデータ伝送方法。

【請求項２２】前記サーバは、伝送するデータをＩＰパケットに変換し、このＩＰパケットを、前記第２の通信経路を介して前記クライアントに伝送する請求項２１に記載のデータ伝送方法。

【請求項２３】前記サーバは、前記ＩＰパケットからメディアアクセス制御（ＭＡＣ）によってＭＡＣフレームを生成し、このＭＡＣフレームを、前記第２の通信経路を介して前記クライアントに伝送する請求項２２に記載のデータ伝送方法。

【請求項２４】前記サーバは、前記ＩＰパケットを暗号化し、暗号化された１個の前記ＩＰパケットについて、１個の前記ＭＡＣフレームを生成する請求項２３に記載のデータ伝送方法。

【請求項２５】前記ＭＡＣフレームのヘッダには、

データを受け取るべきクライアントのＩＰアドレスと、

データの暗号化の有無を示す制御ビットと、

データが、クライアントからの要求に応じたメディアデータであるか、あるいはシステム運用のための制御データであるかを区別するための制御ビットと、

データを暗号化するのに必要となるデータ長の正規化を行なった際の付加データ長を示すビットとが含まれる請求項２３に記載のデータ伝送方法。

【請求項２６】前記サーバは、

要求を出した前記クライアントに配信するＩＰパケットを、当該サーバおよび当該クライアントのみが知る固有の暗号化アルゴリズムによって暗号化する手段と、

メディアアクセス制御を用いて、前記暗号化されたＩＰパケットからＭＡＣフレームを作成する手段と、

前記ＭＡＣフレームをＭＰＥＧ２で規定されたセクションに変換する手段と、

前記セクションを、ＭＰＥＧ２で規定されたトランスポートストリームに変換する手段と、

前記トランスポートストリームを前記第２の通信経路を介して前記クライアントに伝送する手段とを有する請求項２２に記載のデータ伝送方法。

【請求項２７】前記サーバおよび前記クライアントは、ＣＲＣ方式によって、前記ＭＡＣフレームの全データバイトを検査する手段をさらに有する請求項２３に記載のデータ伝送方法。

【請求項２８】前記サーバは、ＭＡＣフレームについてのＣＲＣ検査ビットを、ＭＡＣフレームの最後に付加する手段をさらに有する請求項２３に記載のデータ伝送方法。

【請求項２９】前記サーバは、ＭＡＣフレームについてのＣＲＣ検査ビットを、ＭＡＣフレームの最後に付加する手段をさらに有する請求項２７に記載のデータ伝送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば、通信衛星を用いて、マルチメディアデータ配信サービスを行うためのデータ伝送装置およびその方法に関する。

【０００２】

【従来の技術】従来、テレビ放送などの通信衛星を用いたデータ配信サービスでは、データの流れは、データ配信者からユーザへの一方向のみであった。近年、通信衛星を用いたデジタルデータの伝送が可能になったことで、テレビや映画などのアナログ映像・音声データのみならず、コンピュータなどで利用されるテキストやデジ

タル映像・音声データについても、通信衛星を用いて伝送されるようになった。ここで、テレビ放送などの通信衛星を使った従来のデータ配信サービスは、データ配信者が配信したデータを同時に多数のユーザが受信して使用する形態である。これに対して、コンピュータなどで使用されるディジタルデータを、通信衛星を介して配信する場合には、データ配信者から単数または複数の特定のユーザにデータを配信する機能が求められる。

【０００３】

【発明が解決しようとする課題】しかしながら、通信衛星を用いた従来の伝送方式では、アナログデータの配信であることや、データ配信はデータ配信者からユーザへの一方向のみであることから、伝送上のエラーをチェック機能は備えておらず、データ伝送の信頼性が低いという問題がある。ディジタルデータの配信では、伝送によってデータに１ビットでも誤りが生じると、受信したデータは無意味なものになってしまう。このようなデジタルのコンピュータデータを無線方式で高品質に配信するためには、データ配信者からユーザへの一方向のデータ配信だけでなく、ユーザからデータ配信者への通信路を確保する必要があるが、従来の伝送方式では、このような機能を備えていない。

【０００４】また、従来のデータ配信者から多ユーザへの同時通信又は放送システムでは、全ユーザは常に同じ情報を受信して使用または閲覧をしており、システムユーザ個人の識別情報がないため、データ配信者から特定ユーザのみへのデータの配信ができないという問題がある。

【０００５】本発明は上述した従来技術の問題点に鑑みてなされ、伝送上のエラーを発生させることなく、ディジタルデータを無線方式で伝送できるデータ伝送装置およびその方法を提供することを目的とする。また、本発明は、特定のクライアントのみに、ディジタルデータを無線方式で伝送できるデータ伝送装置およびその方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】上述した目的を達成するために、本発明のデータ伝送装置は、サーバとクライアント間で双方向のデータ伝送が可能な第１のデータ通信経路と、前記サーバからクライアントにデータを無線方式で伝送可能で、前記第１のデータ通信経路に比べて伝送容量が大きな第２のデータ通信経路とを有し、前記サーバは、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第２のデータ通信経路を介して前記クライアントに伝送する。

【０００７】また、本発明のデータ伝送方法は、サーバとクライアント間で双方向のデータ伝送が可能な第１のデータ通信経路と、前記サーバからクライアントにデータを無線方式で伝送可能で、前記第１のデータ通信経路に比べて伝送容量が大きな第２のデータ通信経路とを有するネットワークを介してサーバとクライアント間のデータ伝送を行うデータ伝送方法であって、前記サーバは、複数のシステム相互間でネットワークを介してディジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第２のデータ通信経路を介して前記クライアントに伝送する。

【０００８】本発明のデータ伝送装置およびその方法では、例えばクライアントが第１のデータ通信経路を介して所定のリクエストをサーバに行うと、サーバにおいて、当該リクエストに応じたデータをインターネットプロトコルに基づいて変換し、この変換したディジタルデータを第２のデータ通信経路を介してクライアントに伝送する。

【０００９】本発明によるデータ伝送装置およびその方法によれば、サーバからクライアントに大容量なディジタルデータを高品質に伝送が可能となり、さらに、サーバから特定のユーザにのみディジタルデータの転送が可能となる。

【００１０】

【発明の実施の形態】本発明の実施形態に係わるデータ伝送装置（情報提供システム）およびその方法について説明する。図１に、マルチメディアのデジタルデータ（映像、音声、テキスト等）を配信するデータサービスを実現するためのデータ伝送装置の概略を示す。図１に示すデータ伝送装置では、データ提供者Ａはサーバとしてのデータ配信装置４を所有し、ユーザＢはクライアントとしてのデータ受信装置５を所有している。データ配信装置４およびデータ受信装置５は、双方向の通信が可能なＩＳＤＮ３を介して相互に通信が可能である。また、データ配信装置４から、データ受信装置５へは、通信衛星２を介して、無線方式で大容量の通信が可能である。

【００１１】図１に示すデータ伝送装置におけるデータの流れを説明する。ユーザ提供者ＡとユーザＢが、マルチメディアデータの配送の契約を予め結んでいるものとする。この際、ユーザＢのデータ受信装置５にはデータ提供者Ａのデータ配信装置４からデータを受信できる機能が備わっているとする。さらに、データ提供者Ａは、予めユーザＢとの契約が結ばれていることを知っている。

【００１２】先ず、ユーザＢは、例えば、地上通信網としてのＩＳＤＮ３を介して、データ提供者Ａが提供する所定のサービスを受けたい旨のリクエスト６をデータ提供者Ａに送る。このリエスト６を送る方法は、特に限定されず、データの種類やユーザとの契約状況によって決められ、例えば郵便などでもよい。また、リクエスト６を送らずに、予め契約に従って、データ提供者Ａがサー

ビスを提供してもよい。

【００１３】データ配信装置４に送られたユーザＢからのリクエスト６は、データリクエスト受付部７で受け取られ、データ管理部９に送られる。データ管理部９は、ユーザＢの契約情報やリクエスト６が意味のあるものか否かのチェックを行ない、問題が無ければ、データ貯蓄部１１にデータの読み出し要求１０を行なう。データ貯蓄部１１は、データ読み出し要求１０に応じた、例えばマルチメディアデータ１２をデータ作成部１３へ送る。データ作成部１３では、データ貯蓄部１１からのマルチメディアデータ１２に対してＩＰパケット化、予めユーザＢに対して固有に決められた暗号化、ＭＡＣ（Media Access Control）フレーム化、ＭＰＥＧ(Moving Picutre Experts Group)２のトランスポート化などのデータのフォーマット変換が行なわれる。このデータフォーマット変換についての後述する。

【００１４】データ貯蓄部１１からのマルチメディアデータ１２は、データ作成部１３によって作成又はフォーマット変換された後、データ１４として通信衛星２に送られる。通信衛星２を介して送られたデータ１４は、ユーザＢのデータ受信装置５に限らず、データを受信できる状況にある全てのユーザが受信することが可能である。データ受信装置５は、通信衛星２からの全データを受信し、その中から、自分が出したリクエスト６に応じたデータを選別して受け取る。

【００１５】すなわち、データ受信装置５は、リクエスト６に応じた送信されたデータを含む多数のデータ１４をデータ受信部１６で受信する。データ受信装置５は、その中から、自分宛のデータ、自分が受け取るべきデータ、自分が受けるとることができるデータ（これは契約にもよる）を選別をする。この選別は、データ受信装置５のデータ選択部１８において行われる。尚、予めユーザＢとデータ提供者Ａとの契約によって、ユーザＢが持つデータ受信装置５は決定されている。従って、ユーザＢが持つデータ受信装置５を用いて、他のユーザ宛の特有のデータは選別することができない。

【００１６】データ選択部１８において、ユーザＢが受け取ることが可能なデータ１９は全てデータ分解部２０に送られる。データ分解部２０に送られたユーザＢ宛のデータは、分解もしくは復号されてマルチメディアデータ２１となり、データ実行部２２へ送られる。これによってユーザＢのみが、ユーザＢがリクエストしたユーザＢ宛のデータを受取ることができ、このデータサービスが完了する。尚、リクエストしたデータの受信は、一瞬のうち行われる場合と、長期間にわたって続けられる場合がある。長期間にわたって受信し続ける種類のデータであった場合には、ユーザＢのデータ受信装置５内で、データの受信が引き続き繰り返されることになる。これは、ユーザＢがリクエストしたデータの種類によって状況が変わる。以上が、本発明によるデータ伝送装置の一連のデータの流れである。

【００１７】データ配信装置４

次に、データ配信装置４における、配信データのデータフォーマット変換について詳細に説明する。先ず、図２を参照しながら、データ提供者Ａのデータ配信装置４のデータ作成部１３について説明する。データ配信装置４内のデータ貯蓄部１１には、ユーザが必要とするマルチメディアデータが何も加工されていないかたちで蓄積されている。データ管理部９から、データの読み出し要求１０がユーザＢから来たことを知らされたデータ貯蓄部１１は、リクエストされたマルチメディアデータ１２およびユーザＢのあて先情報３０を同時にデータ作成部１３内のＩＰパケット作成部３１に送る。ここでユーザＢのあて先情報３０とは、ＩＰパケット送信に必要なＩＰアドレスである。本実施形態に係わるデータ伝送装置は、すべての契約ユーザに固有のＩＰアドレスを割り振ってある。ユーザＢが持つＩＰアドレスは、ユーザＢが確保している間は、ユーザＢ以外のユーザは持たない。

【００１８】データ貯蓄部１１から送られたユーザＢ宛のマルチメディアデータ１２およびＩＰアドレス３０はＩＰパケット作成部３１に送られる。ＩＰパケット作成部３１では、データ貯蓄部１１から送られてきたマルチメディアデータ１２とその時点でユーザＢを特定するＩＰアドレス３０を用いて、ＩＰパケット３２を生成する。このＩＰパケットの大きさはＴＣＰ／ＩＰ(Transmission Control Protocol/Internet Protocol）で規定され、ユーザＢがリクエストしたマルチメディアデータがその大きさを超える場合には、このマルチメディアデータは複数のＩＰパケットに分割されて次の暗号部３３に転送される。

【００１９】本実施形態に係わるデータ伝送装置において使用されるＩＰパケット３２のフォーマットを図４に示す。ＩＰパケット内のＩＰヘッダ内の各制御ビットの詳しい説明はここでは省略する。ただし、ＩＰケット内の送信先ＩＰアドレス６１のエリアにはユーザＢのデータ受信装置５が持つＩＰアドレスが入り、送信元ＩＰアドレス６０のエリアにはデータ提供者Ａのデータ配信装置４のＩＰアドレスが入る。さらに、図４内のデータ部５３には図２におけるデータ貯蓄部１１からのマルチメディアデータ１２が入る。

【００２０】図２に示すＩＰパケット作成部３１で作成されたＩＰパケット３２は、暗号部３３に転送される。暗号部３３では、ＩＰパケット３２内の送信先ＩＰアドレス６１によって、あて先がユーザＢであることを知り、その時点で既にデータ提供者ＡとユーザＢとの間のみで知りあう秘密鍵によってＩＰパケット全体３２を暗号化する。暗号化方式としては、例えばＤＥＳ(Data Encryption Standard)などが採用される。ここで、ＩＰパケット３２のヘッダにはユーザＢのみが用いるＩＰアドレスが含まれるのでユーザＢ専用の秘密鍵で暗号化する

必要はないように思われるが、これは他人がユーザＢのＩＰアドレスを用いてユーザＢに成り済ましてユーザＢ宛のデータを盗用することを防ぐために必要となる。

【００２１】ただし、暗号化はユーザＢに対する全てのデータを暗号化するわけではなく、データの種類によっては暗号化が行なわれないこともある。暗号化が行われない場合には、ＩＰパケット作成部３１からＭＡＣフレーム作成部３６に直接ＩＰパケット３２が転送される。本実施形態では、暗号化が行なわれる場合について述べる。暗号化は通常６４ビットの平文に対して行なわれ、暗号化すべきＩＰパケット３２のデータ長が６４ビットの倍数でない場合には、データの埋め合わせ、すなわち、無効データのパッディングを行うことでＩＰパケット全体を６４ビットの倍数にする。

【００２２】ユーザＢ宛のＩＰパケット３２全体が暗号化されたパケットデータ３５は、ＭＡＣフレーム作成部３６に転送される。ＭＡＣフレーム３７のフォーマットを図５に示す。ＭＡＣフレーム作成部３６では、暗号部３３によって暗号化されたユーザＢ宛のＩＰパケット３５に対して、図５に示す通りのＭＡＣヘッダ１１９を付加する。ＭＡＣヘッダ１１９内の送信先ＩＰアドレス５４はユーザＢが持つＩＰアドレスである。ここで、ＭＡＣヘッダ１１９の送信先ＩＰアドレス５４と、暗号化されたＩＰパケット３５内の送信先ＩＰアドレスとは同じである。このように、ＭＡＣヘッダ１１９を付けるのは、データ受信装置５はデータ受信時において、ＭＡＣヘッダ１１９からのみ送信先ＩＰアドレスを知ることができるためである。すなわち、データ受信装置５は、暗号化されたＩＰパケット３５全体を復号するまでユーザＢは送信先アドレスを見ることができないため、暗号化されたパケット３５のみでは、自分宛のパケットかどうかを識別できない。従って、データ受信装置５が、受信したＩＰパケットを復号する前に、そのＩＰパケットが自分宛のものであることを知るために、ＭＡＣフレームのヘッダに送信先ＩＰアドレス５４がセットされる必要がある。この送信先ＩＰアドレス５４は、ＩＰパケット作成部３１からＭＡＣフレーム作成部３６に直接渡される。

【００２３】また、図５に示すＭＡＣヘッダ１１９内のＰＢＬ５５はパッディングバイト長であり、暗号化の際に埋め合わせされた無効なデータの長さである。これは、暗号化されたＩＰパケットを受信したユーザが正規なデータ長を知るために必要となる。また、ＣＰ５６は、ＩＰパケットに、ユーザが必要なマルチメディアデータかシステム運用に必要な制御データが入っているかを識別するビットである。通常、ユーザがリクエストした際に受け取るべきＭＡＣフレーム３７のＣＰ５６は、制御データでなくマルチメディアデータが入っていることを示している。ＭＡＣヘッダ１１９内のＥＮ５７は、ＩＰパケットが暗号部３３によって暗号化されたかどうかを示す制御ビットである。このビット情報によってユーザは受信したＭＡＣフレーム３７を復号をするかしないか決定する。図２のＭＡＣフレーム作成部３６では、以上の制御ビットが暗号化された（場合によっては暗号化はされない）ＩＰパケット３５に付加される。

【００２４】図２のＭＡＣフレーム作成部３６で生成されたＭＡＣフレーム３７は、ＣＲＣ計算部３８に転送される。ＣＲＣ計算部３８では、送れられてきたＭＡＣフレーム３７全バイトのＣＲＣ（Cyclic Redundancy Checking：巡回冗長検査）の計算を行う。本実施形態では、ＣＲＣは１６ビットである。このようにＣＲＣの計算を行うことで、データ受信装置５は、受信したＭＡＣフレームが正しく通信衛星２から伝送されているかを検査することができる。ＣＲＣ計算部３８において生成された１６ビットのＣＲＣ３８ａは、図３，図５に示すように、ＭＡＣフレーム３７の最後に付加される。

【００２５】ＣＲＣ３８ａが付加されたＭＡＣフレーム３９は、セクション作成部４０に転送されてＭＰＥＧ２で規定されるセクションに変換される。図３に示すように、ＭＡＣフレーム３９は、セクションヘッダ（ＳｅｃＨｄ）１２０の直後に付加される。セクションヘッダ１２０のフォーマットを図６（Ａ）に示す。図６（Ａ）で示したセクションヘッダ１２０のフォーマットは、ＭＰＥＧ２によって規定され、テーブルｉｄ１００、セクションーシンクーインディケータ１０１、プライベートーインディケータ１０２、リザーブド１０３、プライベートーセクションーレングス１０４を有する。ここで、プライベートーセクションーレングス１０４には、ＭＡＣフレーム３９のデータ長が入る。

【００２６】図２に示すセクション作成部４０で作成されたセクション４１は、トランスポートパケット作成部４２に転送される。トランスポートパケット作成部４２では、転送されたセクションフォーマットデータをトランスポートパケット４３に分割して次のデータ転送部４４に転送する。

【００２７】図３に示すトランスポートパケット４３のパケットヘッダ（ＴＳＨｄ）１２１のフォーマットを図６（Ｂ）に示す。トランスポートパケット４３のヘッダフォーマットはＭＰＥＧ２で規定されている。図６（Ｂ）に示すように、トランスポートパケット４３のパケットヘッダ１２１は、シンクバイト１１０、トランスポートーエラーーインディケータ１１１、ペイロードーユニットースタートーインディケータ１１２、トランスポートープライオリティ１１３、ＰＩＤ１１４、トランスポートースクランブルーコントロール１１５、アダプテイションーフィールドーコントロール１１６およびコンティニティーカウンタ１１７を有する。トランスポートパケット４３の１個分の大きさは１８８バイトと規定されているので、一般的に、一つのセクション４１を複数のトランスポートパケット４３に分割する必要があ

る。

【００２８】ここで、通常、一つのセクションは１８４バイト（１８８バイトからヘッダ長の４バイトを引いたバイト数）の整数倍長とは限らないので、一つのセクション４１を複数のトランスポートパケット４３に分割する際に、図３に示すように、スタッフィングと呼ばれるデータ穴埋めを行い、スタッフィング領域５１を形成する。すなわち、１８４バイトの倍数でない一つのセクション４１を複数のトランスポートパケット４３に分割した場合、最後のトランスポートパケット４３の余ったデータエリアに、全てのビット１がスタッフィングされたスタッフィング領域５１を形成する。

【００２９】このように複数のトランスポートパケット４３に分割されたセクション４１は、データ転送部４４に転送され、マルチプレクサなどのデータ処理部を通った後、通信衛星２に伝送され、ブロードキャストされる。ブロードキャストされたユーザＢのためのマルチメディアデータは、ユーザＢのデータ受信装置５によって受信され、図２で示した逆の処理がデータ分解部２０によって行なわれ、最終的にリクエストされたマルチメディアデータはユーザＢ３の手元に届くこととなる。

データ受信装置５

【００３０】図２に示すユーザＢのデータ受信装置５のデータ分解部２０において行なわれる具体的な処理は、基本的には、データ配信装置４のデータ作成部１３におけうアルゴリズムの逆アルゴリズムである。先ず、図１に示すデータ受信部１６において、通信衛星２を介して受信した図３に示すトランスポートパケット４３を結合してセクション４１を生成する。次に、データ受信部１６は、セクション４１を伸長して、ＭＡＣフレーム３９を生成し、これをデータ選択部１８に出力する。そして、データ選別部１８において、図３に示すＭＡＣフレーム３９のマックヘッダ１１９に含まれる図５に示す送信先ＩＰアドレス５４に基づいて、この送信先ＩＰアドレス５４とデータ受信装置５のＩＰアドレスとが一致するかを判断する。そして、データ選別部１８は、一致するした場合に、当該データを選別し、このデータに含まれる図３に示す暗号化されたＩＰパケット３５を図１に示すデータ１９としてデータ分解部２０に出力する。

【００３１】データ分解部２０では、データ１９として入力した図３に示す暗号化されたＩＰパケット３５を、予めデータ提供者Ａとの間のみを知りあう秘密鍵を用いて複号した後、データ誤り検査などを行う。ここで、例えば、データ誤りがある場合には、データを復帰させる処理を行うか、あるいは、当該誤りのあるデータを破棄する。

【００３２】以上説明したように、本実施形態に係わるデータ伝送装置およびその方法によれば、ＴＣＰ／ＩＰ通信プロトコルを用いると共に、ＩＰパケットにＣＲＣビットを設けることで、データ配信装置４から通信衛星２を介してデータ受信装置５にディジタルデータを伝送した場合でも、データ伝送エラーが発生することを効果的に抑制し、高品質なディジタルデータ転送を実現できる。また、本実施形態に係わるデータ伝送装置およびその方法によれば、ＩＰパケットをＭＡＣフレーム方式で伝送することで、特定のユーザのみにデータを伝送することができる。また、本実施形態に係わるデータ伝送装置およびその方法によれば、伝送されるデータは暗号化されており、データ受信装置５のみが、それを復号化する秘密鍵を持っていることから、当該データが他人に盗用されることを効果的に防止できる。

【００３３】本発明は上述した実施形態には限定されない。例えば、ＭＡＣフレームのデータ圧縮方法は、ＭＰＥＧ２には限定されず、他の圧縮方法を用いてもよい。また、インターネットプロトコルは、ＴＣＰ／ＩＰには限定されず、例えばＯＳＩ(Open Systems Interconnection)方式を用いてもよい。さらに、本実施形態では、暗号化方法として、秘密鍵を用いる場合について例示したが、公開鍵を用いても同様な効果を得ることできる。

【００３４】

【発明の効果】本発明のデータ伝送装置およびその方法によれば、無線方式でデータを送信する場合でも、データ伝送エラーが発生することを効果的に抑制し、高品質なディジタルデータ転送を実現できる。また、本発明のデータ伝送装置およびその方法によれば、ＭＡＣフレーム方式を採用することで、ブロードキャスト型のデータ配信のみならず、単数または複数の特定のユーザのみにデータを無線方式で伝送することができる。また、本発明のデータ伝送装置およびその方法によれば、暗号化されたデータを伝送することで、当該データが他人に盗用されることを効果的に防止できる。また、本発明のデータ配信装置およびデータ受信装置を用いることで、上述したような効果を有するデータ伝送装置を実現できる。

【図面の簡単な説明】

【図１】本発明の実施形態に係わるデータ伝送装置の構成図である。

【図２】図１に示すデータ配信装置の構成図である。

【図３】図２に示すデータ配信装置およびデータ受信装置における処理を説明するための図である。

【図４】ＩＰパケットのフォーマットを説明するための図である。

【図５】ＭＡＣフレームのフォーマットを説明するための図である。

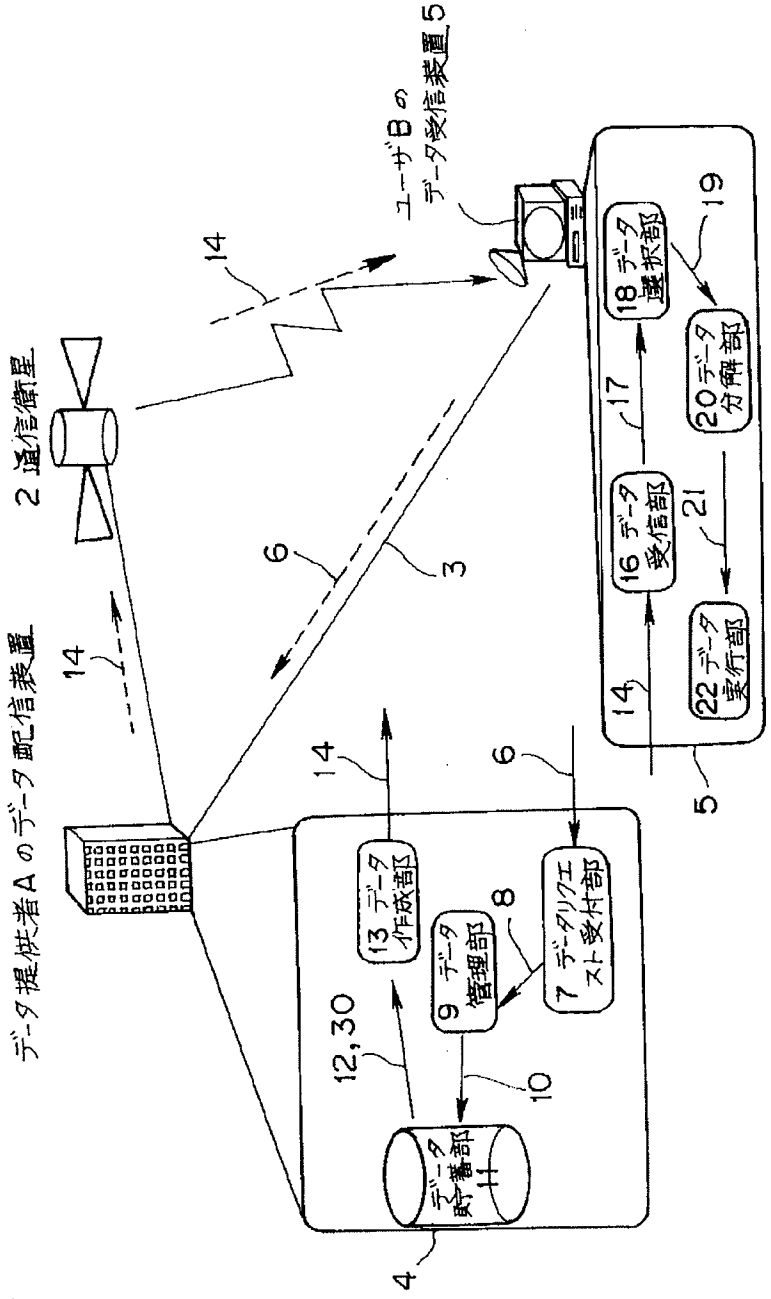
【図６】（Ａ）はセクションヘッダ（ＳｅｃＨｄ）のフォーマットを説明するための図であり、（Ｂ）はトランスポートパケットのパケットヘッダ（ＴＳＨｄ）を説明するための図である。

【符号の説明】

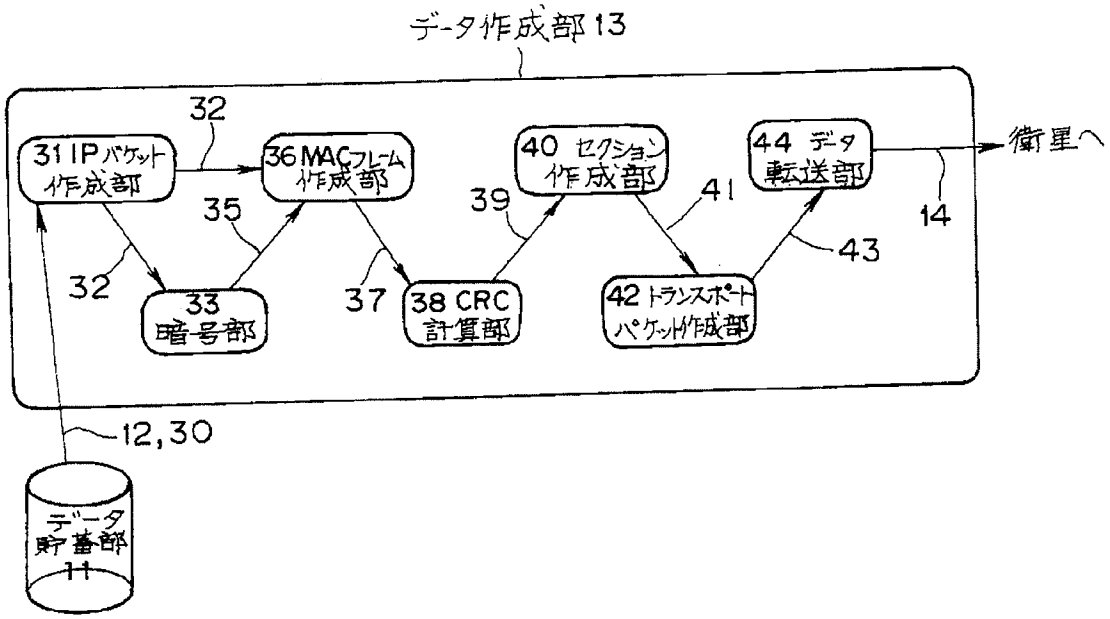
２…通信衛星、３…ＩＳＤＮ、４…データ配信装置、５…データ受信装置、６…リクエスト、７…リクエスト受

付部、９…データ管理部、１０…データ読み出し要求、１１…データ貯蓄部、１２…マルチメディアデータ、１３…データ作成部、１４…無線方式で伝送するデータ、１６…データ受信部、１８…データ選択部、１９…ユーザＢが受け取ることができるデータ、２０…データ分解部、２１…マルチメディアデータ、２２…データ実行部、３１…ＩＰパケット作成部、３３…暗号部、２６…ＭＡＣフレーム作成部、３８…ＣＲＣ計算部、４０…セクション作成部、４２…トランスポートパケット作成部、４４…データ転送部、３２…ＩＰパケット、３５…暗号化されたＩＰパケット、３９…ＭＡＣフレーム、１２０…セクションヘッダ、１２１…トランスポートパケットヘッダ、４３…トランスポートパケット

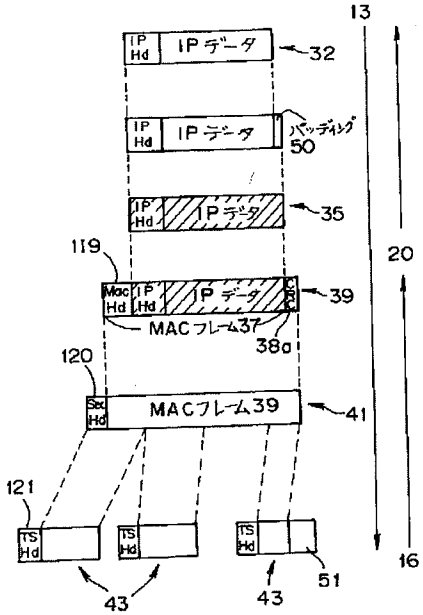
【図１】



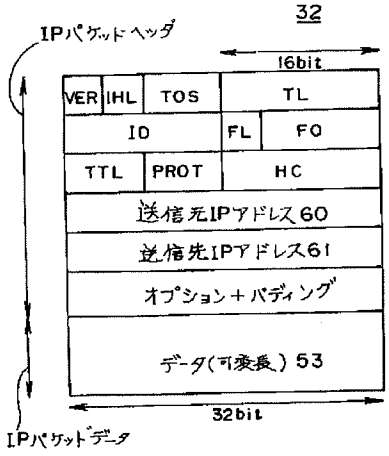
【図2】


データ作成部13
31 IPパケット作成部
32
36 MACフレーム作成部
40 セクション作成部
44 データ転送部
衛星へ
35
39
41
14
43
32
33 暗号部
37
38 CRC計算部
42 トランスポートパケット作成部
12,30
データ貯蓄部
11

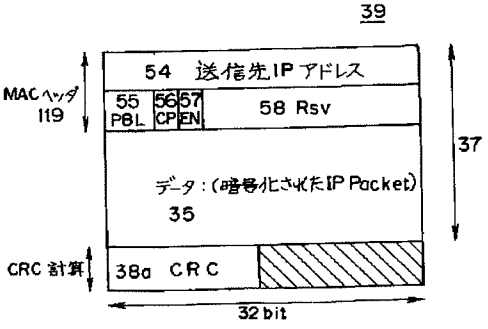
【図3】


13
IP Hd
IPデータ
32
パッディング
50
35
119
Mac Hd
CRC
39
MACフレーム37
38a
120
Src Hd
MACフレーム39
41
121
TS Hd
43
51
20
16

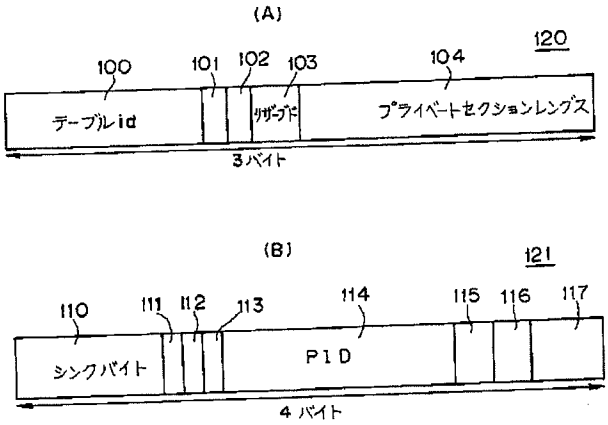
【図4】


IPパケットヘッダ
32
16bit
VER
IHL
TOS
TL
ID
FL
FO
TTL
PROT
HC
送信元IPアドレス60
送信先IPアドレス61
オプション＋パディング
データ(可変長) 53
32bit
IPパケットデータ

【図5】


39
54 送信先IPアドレス
MACヘッダ
119
55 PBL
56 CP
57 EN
58 Rsv
37
データ：(暗号化されたIP Packet)
35
CRC計算
38a CRC
32 bit

【図6】



フロントページの続き

(51) Int.Cl.6	識別記号	庁内整理番号	FI		技術表示箇所
H04H 1/08			H04B 7/26	M	